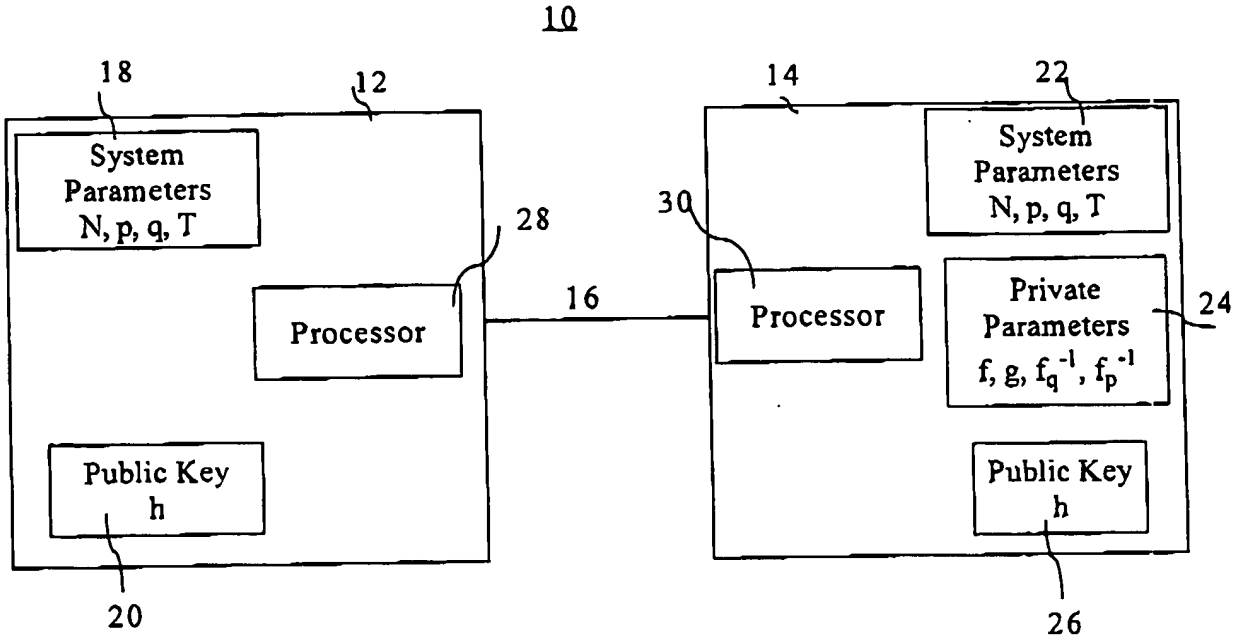

10
18
12
14
22
System Parameters N, p, q, T
28
30
System Parameters N, p, q, T
Processor
16
Processor
Private Parameters f, g, f_q^{-1}, f_p^{-1}
24
Public Key h
Public Key h
20
26

Figure 1

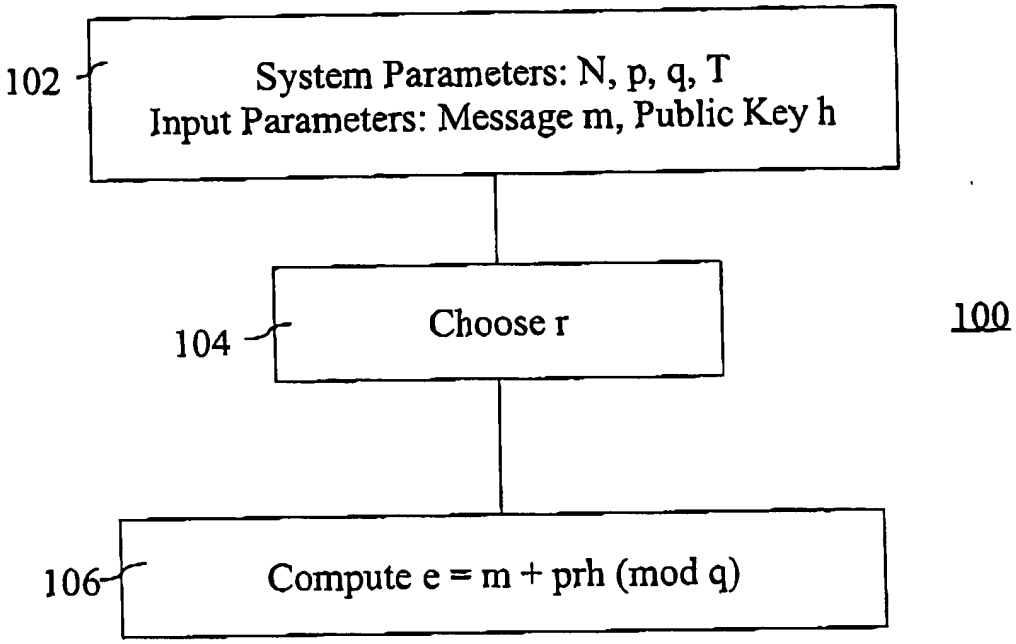

102
System Parameters: N, p, q, T
Input Parameters: Message m, Public Key h
104
Choose r
100
106
Compute e = m + prh (mod q)

Figure 2

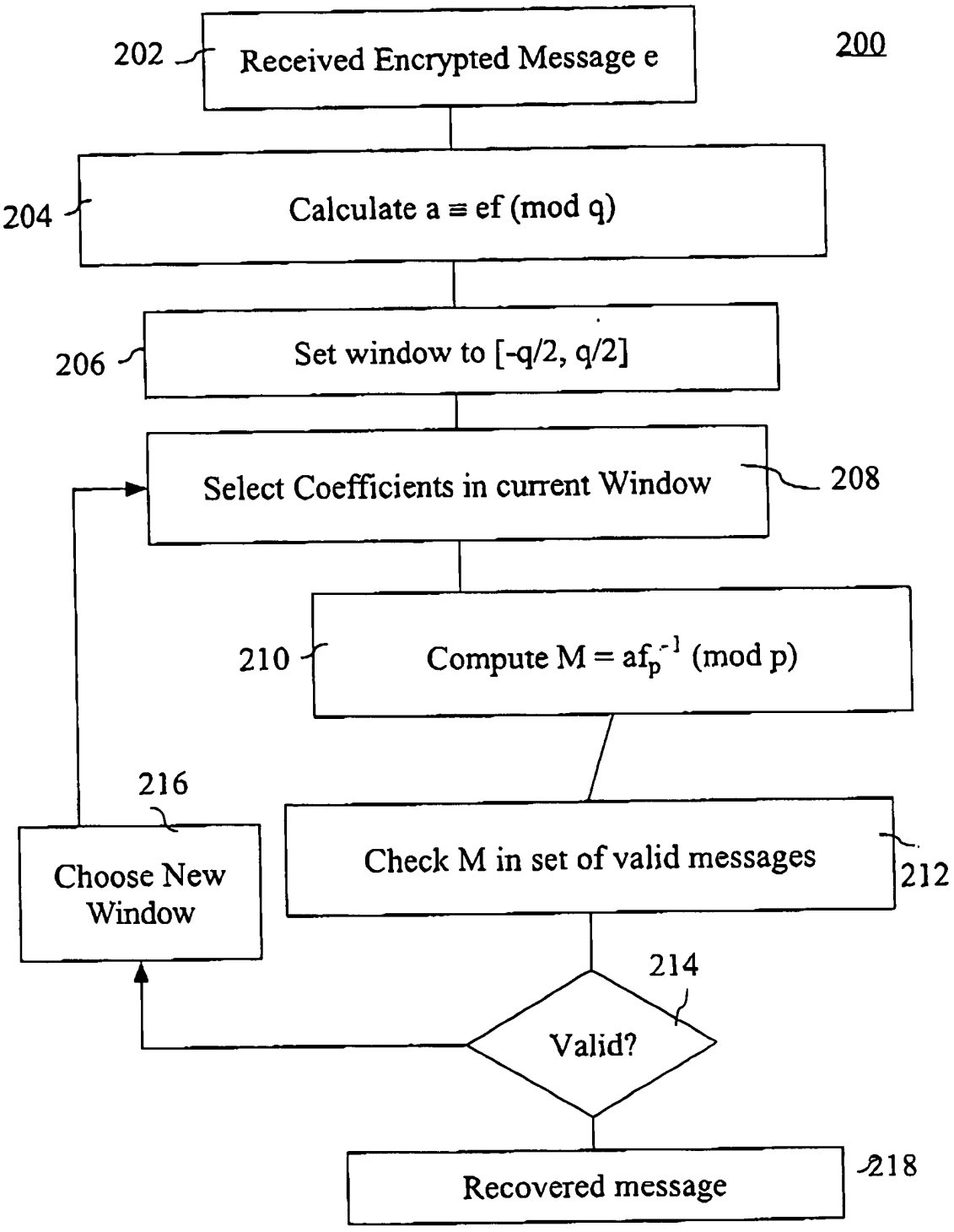

200
202
Received Encrypted Message e
204
Calculate a ≡ ef (mod q)
206
Set window to [-q/2, q/2]
208
Select Coefficients in current Window
210
Compute M = af_p^-1 (mod p)
212
Check M in set of valid messages
214
Valid?
216
Choose New Window
218
Recovered message

Figure 3

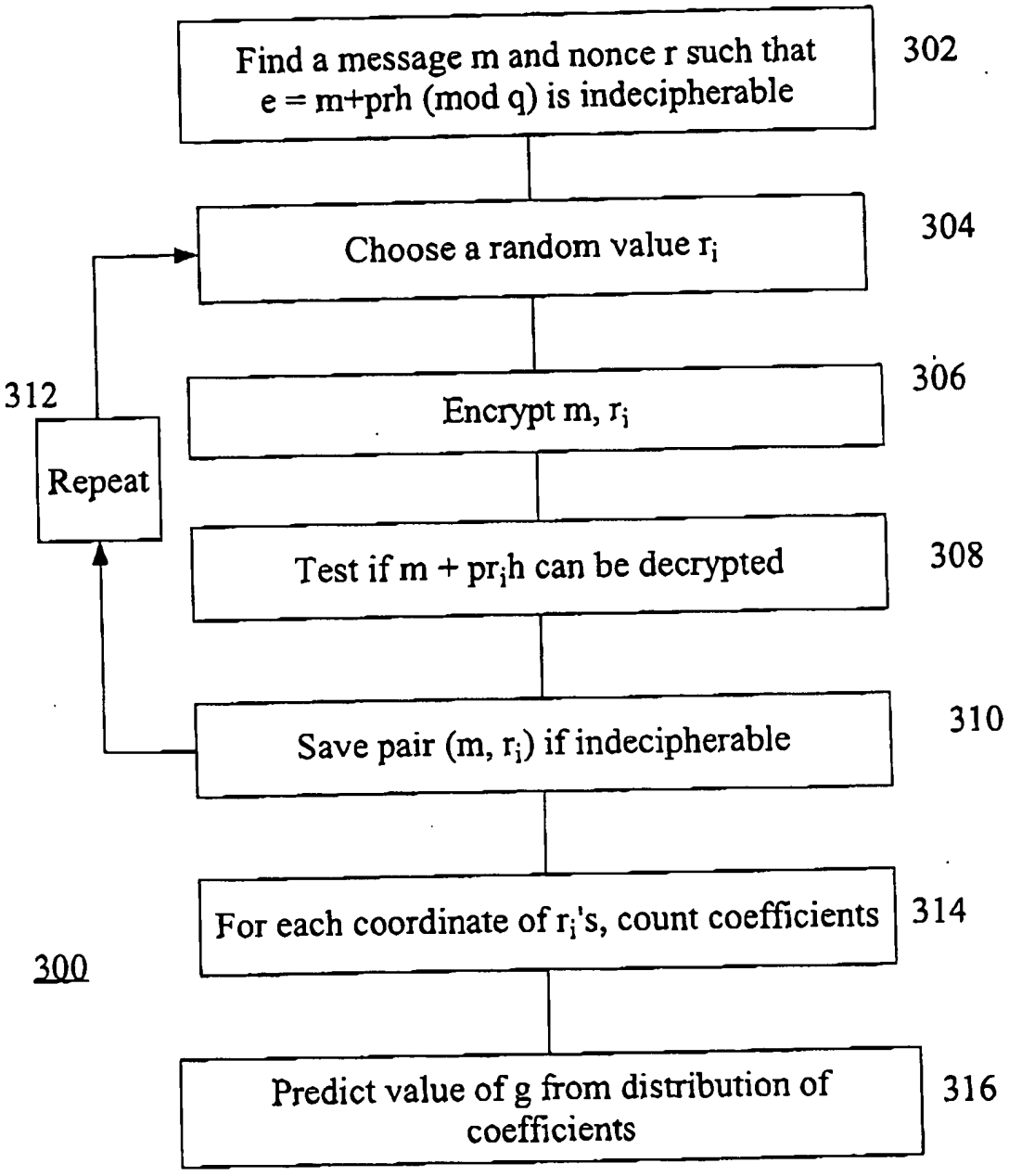

Find a message m and nonce r such that e = m+prh (mod q) is indecipherable
302
Choose a random value r_i
304
Encrypt m, r_i
306
Test if m + pr_ih can be decrypted
308
Save pair (m, r_i) if indecipherable
310
For each coordinate of r_i's, count coefficients
314
Predict value of g from distribution of coefficients
316
Repeat
312
300

Figure 4

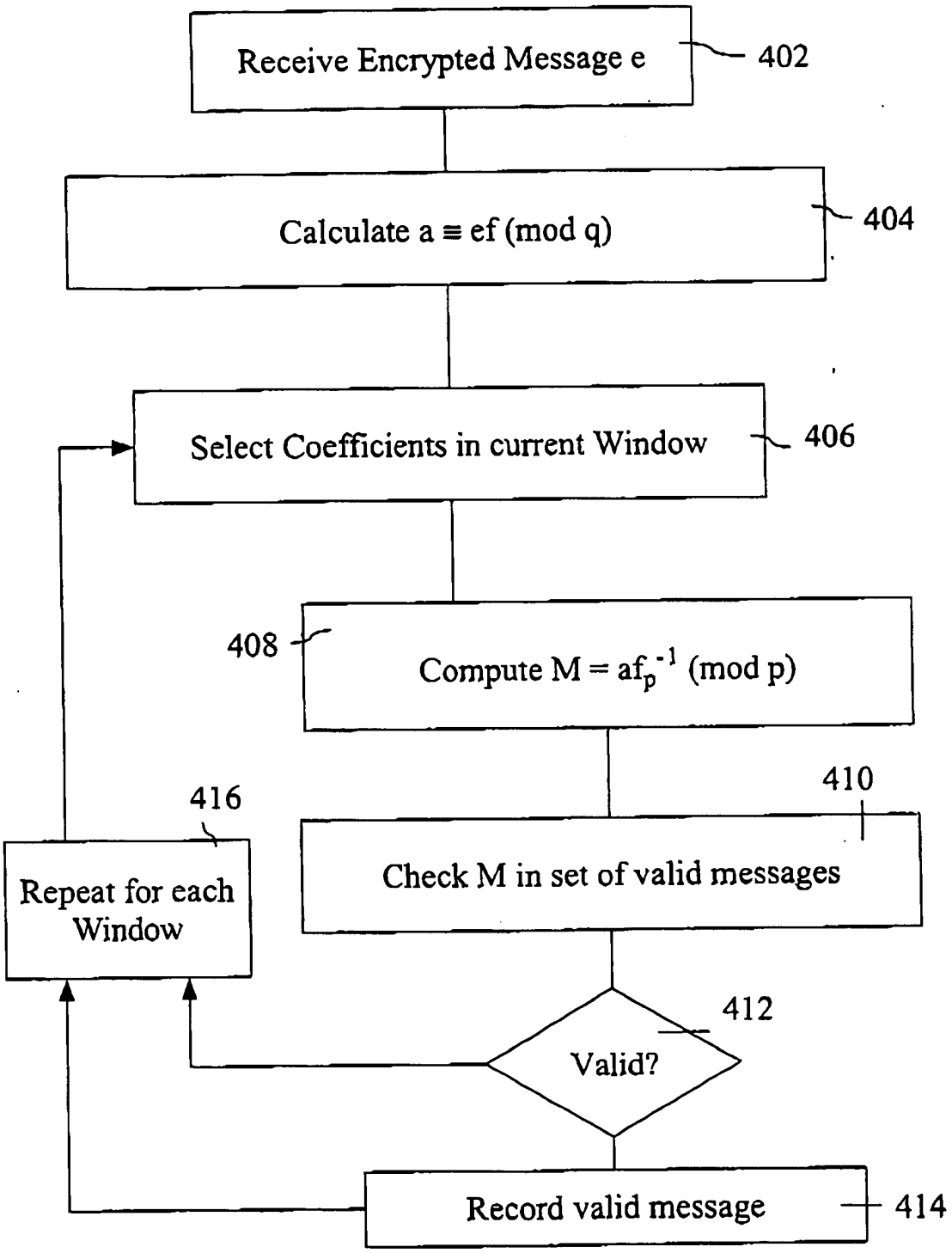

Receive Encrypted Message e
402
Calculate a ≡ ef (mod q)
404
Select Coefficients in current Window
406
408
Compute M = af_p^-1 (mod p)
410
416
Repeat for each Window
Check M in set of valid messages
412
Valid?
Record valid message
414

Figure 5

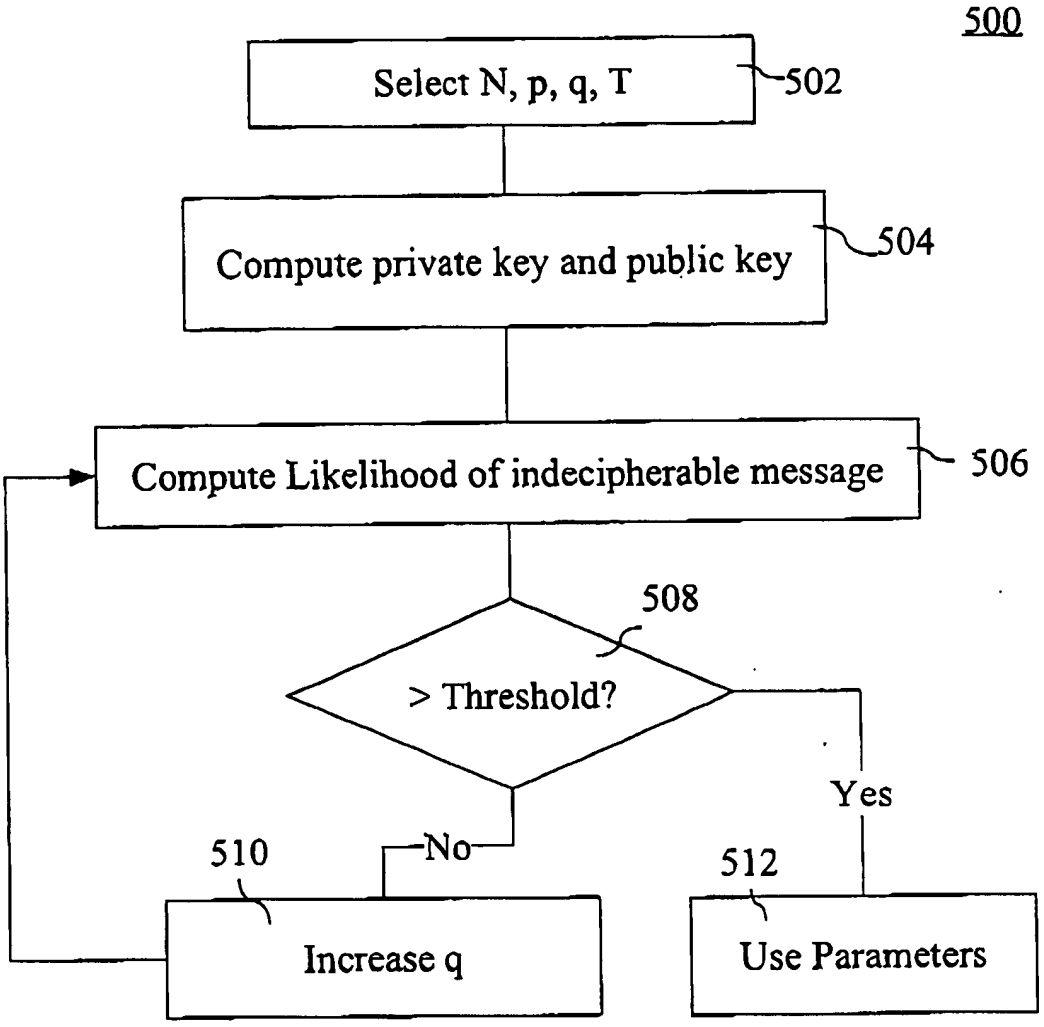

500
Select N, p, q, T
502
Compute private key and public key
504
Compute Likelihood of indecipherable message
506
508
> Threshold?
Yes
No
510
512
Increase q
Use Parameters

Figure 6

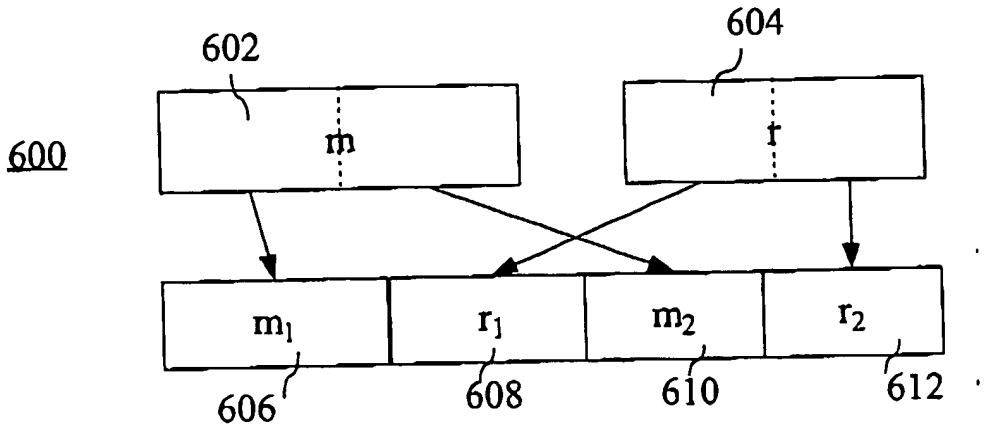


Figure 7

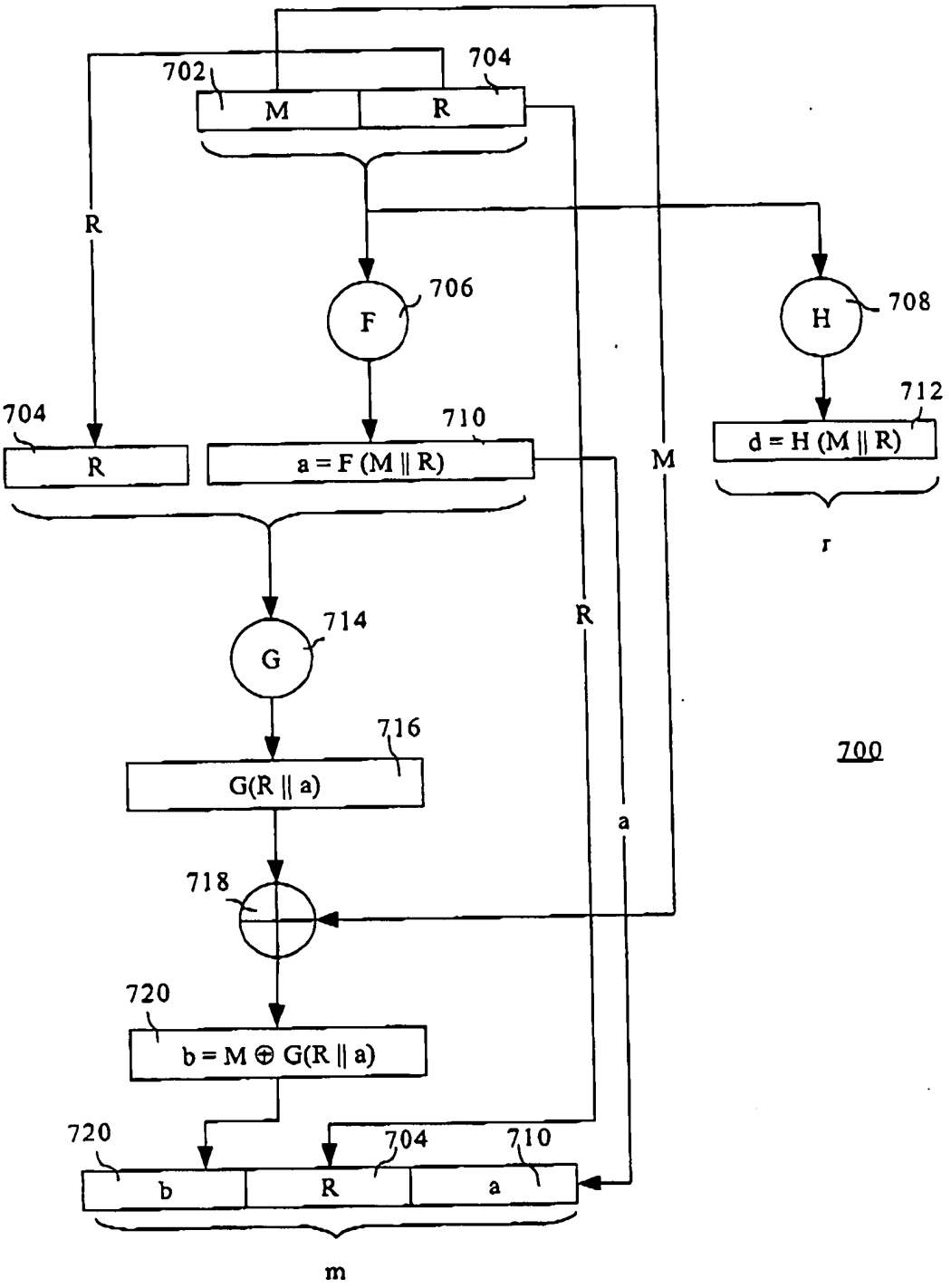

702
704
M
R
R
706
F
H
708
712
704
710
R
a = F (M || R)
M
d = H (M || R)
r
714
G
R
716
G(R || a)
700
a
718
720
b = M ⊕ G(R || a)
720
704
710
b
R
a
m

Figure 8

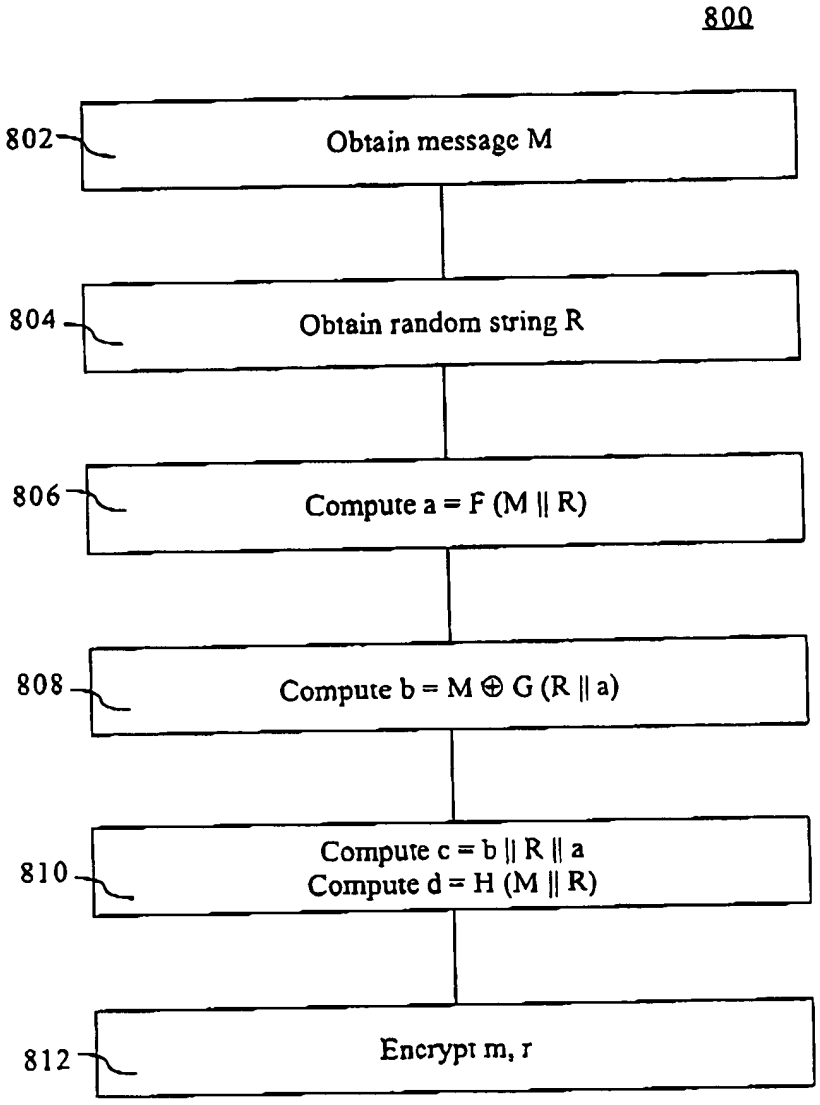

800
802
Obtain message M
804
Obtain random string R
806
Compute a = F (M || R)
808
Compute b = M ⊕ G (R || a)
810
Compute c = b || R || a
Compute d = H (M || R)
812
Encrypt m, r

Figure 9

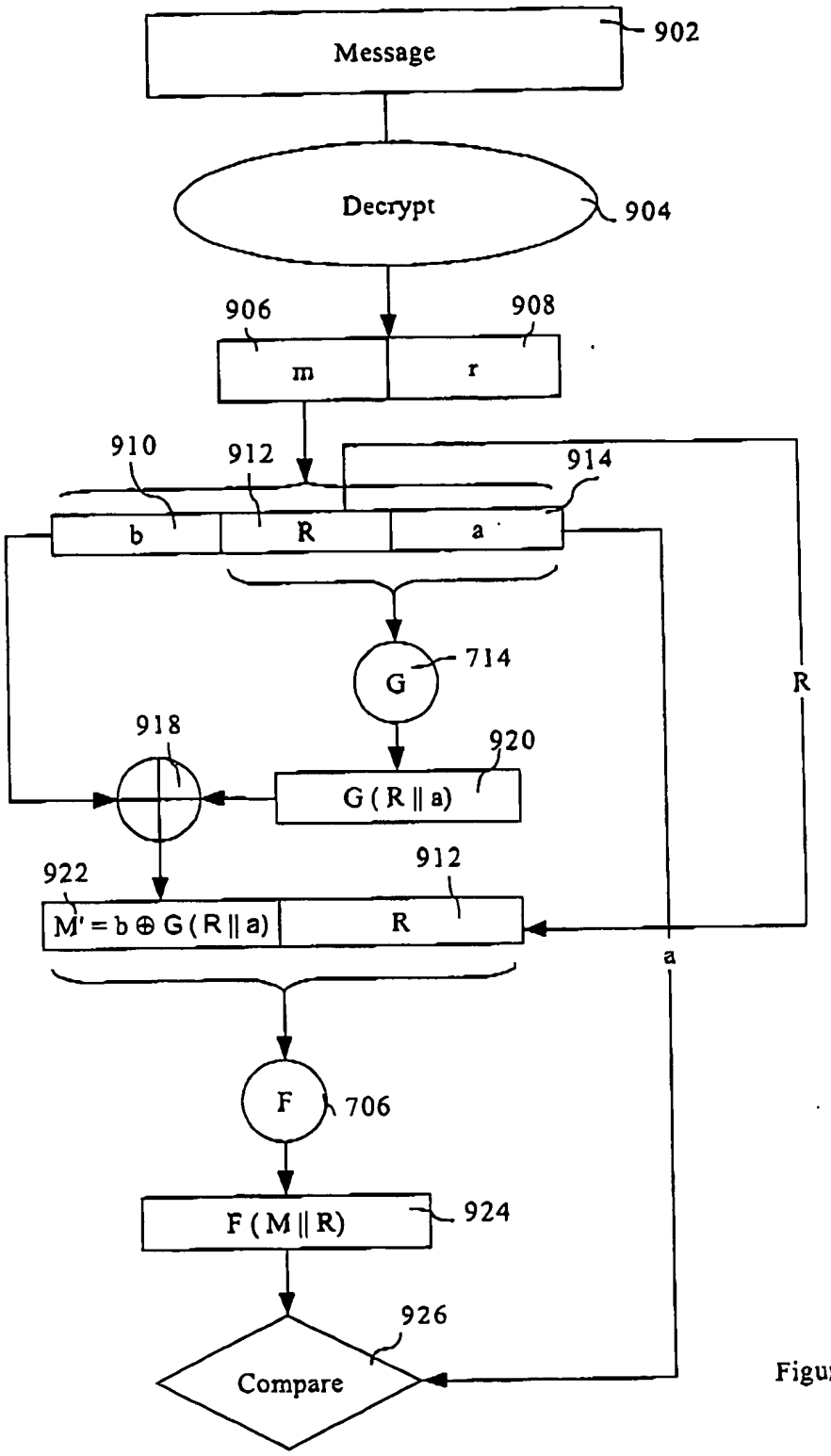

Message
902
Decrypt
904
900
906
908
m
r
910
912
914
b
R
a
G
714
R
918
920
G (R || a)
922
912
M' = b ⊕ G (R || a)
R
a
F
706
F (M || R)
924
926
Compare

Figure 10

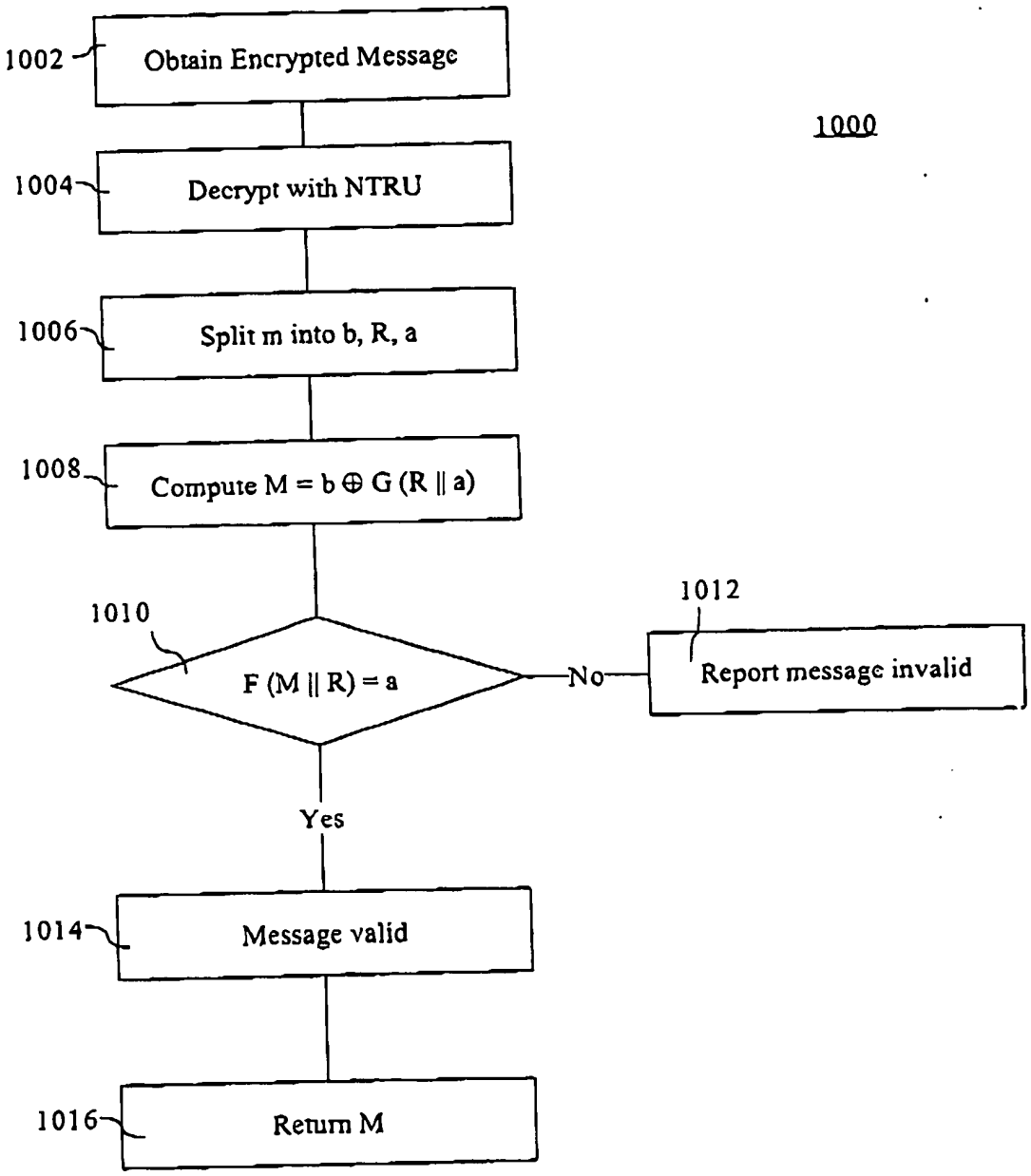

1000
1002
Obtain Encrypted Message
1004
Decrypt with NTRU
1006
Split m into b, R, a
1008
Compute M = b ⊕ G (R || a)
1010
F (M || R) = a
No
1012
Report message invalid
Yes
1014
Message valid
1016
Return M

Figure 11